IN THE CLAIMS

A list of the pending claims is presented below.

1. (Previously Presented) A method of controlling information flow through a firewall, said method comprising:

determining a first incoming packet community set (PCS) of a first data packet received on an interface of said firewall;

discarding said first data packet in response to detecting said first incoming PCS is not a subset of an interface community set (IFCS) of said interface; and

processing said first data packet in response to detecting said first incoming PCS is a subset of said IFCS, wherein said processing comprises:

matching said first data packet to a first rule of a plurality of rules of said firewall;

comparing said first incoming PCS to a second incoming PCS specified by the first rule;

changing the first incoming PCS in the first data packet to an outgoing PCS specified by the first rule, in response to determining the first incoming PCS matches the second incoming PCS;

comparing said outgoing PCS with a destination community set of said first data packet, prior to transmitting the first data packet to said destination community;

discarding said first data packet in response to detecting said outgoing PCS is not a subset of said destination community set; and

further processing said first data packet in response to detecting said outgoing PCS is a subset of said destination community set;

wherein the determining , discarding, and processing are performed within a single node of a network.

2. (Original) The method of claim 1, wherein said determining comprises determining a source network address community set (NACS) of said first data packet.

3. (Original) The method of claim 1, wherein said determining comprises determining a source network service community set (NSCS) of said first data packet.

4. (Original) The method of claim 1, wherein said incoming PCS is encoded in a header of said first data packet, and wherein said determining comprises decoding said incoming PCS from said header of said first data packet.

5. (Cancelled).

6. (Previously Presented) The method of claim 1, wherein said processing further comprises discarding the first data packet, in response to determining the first incoming PCS does not match the second incoming PCS.

7. (Cancelled).

8. (Previously Presented) The method of claim 6, wherein changing said first incoming PCS to the outgoing PCS is in further response to determining that said first rule includes the action of forwarding said first data packet.

9. (Cancelled).

10. (Previously Presented) The method of claim 1, wherein said destination community set is a network address community set (NACS).

11. (Previously Presented) The method of claim 1, wherein said destination community set is a network service community set (NSCS).

12. (Previously Presented) The method of claim 1, wherein said further processing comprises:

transmitting said first data packet via an output interface of said firewall in response to detecting said outgoing PCS is a subset of the interface community set (IFCS) of said output interface; and

discarding said first data packet in response to detecting said outgoing PCS is not a subset of said IFCS.

13. (Previously Presented) The method of claim 12, wherein said further processing further comprises encoding said outgoing PCS in a header of said first data packet.

14. (Original) The method of claim 13, further comprising recording an event corresponding to said first data packet in response to detecting said outgoing PCS is not a subset of said destination community set.

15. (Original) The method of claim 1, further comprising consulting a community information base (CIB).

16. (Original) The method of claim 15, wherein said CIB includes community set information corresponding to network addresses, network services, and interfaces.

17. (Original) The method of claim 12, further comprising recording an event corresponding to said first data packet in response to detecting said first data packet is discarded.

18. (Previously Presented) A node configured to act as a firewall, wherein said node comprises:

a processing unit, wherein said processing unit is configured to:

determine a first incoming packet community set (PCS) of a first data packet received on an interface of said node;

discard said first data packet in response to detecting said first incoming PCS is not a subset of an interface community set (IFCS) of said interface; and

process said first data packet in response to detecting said first incoming PCS is a subset of said IFCS, wherein processing the first data packet comprises:

matching said first data packet to a first rule of a plurality of rules of said firewall;

comparing said first incoming PCS to a second incoming PCS specified by the first rule;

changing the first incoming PCS in the first data packet to an outgoing PCS specified by the first rule, in response to determining the first incoming PCS matches the second incoming PCS;

compare said outgoing PCS with a destination community set of said first data packet, prior to transmitting the first data packet to said destination community ;

discard said first data packet in response to detecting said outgoing PCS is not a subset of said destination community set; and

process said first data packet for output in response to detecting said outgoing PCS is a subset of said destination community set; and

a community information base coupled to said processing unit.

19. (Original) The node of claim 18, wherein said processing unit is configured to determine said incoming PCS by determining a source network address community set (NACS) of said first data packet.

20. (Original) The node of claim 18, wherein said processing unit is configured to determine said incoming PCS by determining a source network service community set (NSCS) of said first data packet.

21. (Original) The node of claim 18, wherein said incoming PCS is encoded in a header of said first data packet, and wherein said processing unit is configured to determine said incoming PCS by decoding said incoming PCS from said header of said first data packet.

22. (Cancelled).

23. (Previously Presented) The node of claim 18, wherein processing the first data packet further comprises discarding the first data packet, in response to determining the first incoming PCS does not match the second incoming PCS.

24. (Cancelled).

25. (Previously Presented) The node of claim 23, wherein changing said first incoming PCS to the outgoing PCS is in further response to detecting that said first rule includes the action of forwarding said first data packet.

26. (Cancelled).

27. (Previously Presented) The node of claim 18, wherein said destination community set is a network address community set (NACS).

28. (Previously Presented) The node of claim 18, wherein said destination community set is a network service community set (NSCS).

29. (Previously Presented) The node of claim 18, wherein said processing said first data packet for output comprises:

transmitting said first data packet via an output interface of said firewall in response to detecting said outgoing PCS is a subset of the interface community set (IFCS) of said output interface; and

discarding said first data packet in response to detecting said outgoing PCS is not a subset of said IFCS.

30. (Previously Presented) The node of claim 29, wherein said processing unit is further configured to encode said outgoing PCS in a header of said first data packet prior to said transmitting.

31. (Original) The node of claim 30, wherein said processing unit is further configured to record an event corresponding to said first data packet in response to detecting said outgoing PCS is not a subset of said destination community set.

32. (Original) The node of claim 18, wherein said processing unit is configured to consult said community information base (CIB).

33. (Original) The node of claim 32, wherein said CIB includes community set information corresponding to network addresses, network services, and interfaces.

34. (Original) The node of claim 29, further comprising recording an event corresponding to said first data packet in response to detecting said first data packet is discarded.

35. (Previously Presented) A computer network comprising:

a node configured to act as a firewall, wherein said node comprises:
a processing unit, wherein said processing unit is configured to:
determine a first incoming packet community set (PCS) of a first data packet received on an interface of said node;

discard said first data packet in response to detecting said first incoming PCS is not a subset of an interface community set (IFCS) of said interface; and

process said first data packet in response to detecting said first incoming PCS is a subset of said IFCS, wherein processing the first data packet comprises:

matching said first data packet to a first rule of a plurality of rules of said firewall;

comparing said first incoming PCS to a second incoming PCS specified by the first rule; and

changing the first incoming PCS in the first data packet to an outgoing PCS specified by the first rule, in response to determining the first incoming PCS matches the second incoming PCS;

comparing said outgoing PCS with a destination community set of said first data packet, prior to transmitting the first data packet to said destination community;

discarding said first data packet in response to detecting said outgoing PCS is not a subset of said destination community set; and

further processing said first data packet in response to detecting said outgoing PCS is a subset of said destination community set;

and

a community information base coupled to said processing unit;

a first computer network coupled to said node; and

a second computer network coupled to said node.

36. (Original) The computer network of claim 35, wherein said node is configured to determine said incoming PCS by determining a source network address community set (NACS) of said first data packet.

37. (Original) The computer network of claim 35, wherein said node is configured to determine said incoming PCS by determining a source network service community set (NSCS) of said first data packet.

38. (Original) The computer network of claim 35, wherein said incoming PCS is encoded in a header of said first data packet, and wherein said node is configured to determine said incoming PCS by decoding said incoming PCS from said header of said first data packet.

39. (Cancelled).

40. (Previously Presented) The computer network of claim 35, wherein processing the first data packet further comprises discarding the first data packet, in response to determining the first incoming PCS does not match the second incoming PCS.

41. (Cancelled).

42. (Previously Presented) The computer network of claim 40, wherein changing said first incoming PCS to the outgoing PCS is in further response to detecting that said first rule includes the action of forwarding said first data packet.

43. (Cancelled).

44. (Previously Presented) The computer network of claim 35, wherein said destination community set is a network address community set (NACS).

45. (Previously Presented) The computer network of claim 35, wherein said destination community set is a network service community set (NSCS).

46. (Previously Presented) The computer network of claim 35, wherein said processing said first data packet for output comprises:

transmitting said first data packet via an output interface of said firewall in response to detecting said outgoing PCS is a subset of the interface community set (IFCS) of said output interface; and

discarding said first data packet in response to detecting said outgoing PCS is not a subset of said IFCS.

47. (Previously Presented) The computer network of claim 46, wherein said node is further configured to encode said outgoing PCS in a header of said first data packet prior to said transmitting.

48. (Original) The computer network of claim 47, wherein said node is further configured to record an event corresponding to said first data packet in response to detecting said outgoing PCS is not a subset of said destination community set.

49. (Original) The computer network of claim 35, wherein said node is configured to consult said community information base (CIB).

50. (Original) The computer network of claim 49, wherein said CIB includes community set information corresponding to network addresses, network services, and interfaces.

51. (Original) The computer network of claim 46, further comprising recording an event corresponding to said first data packet in response to detecting said first data packet is discarded.